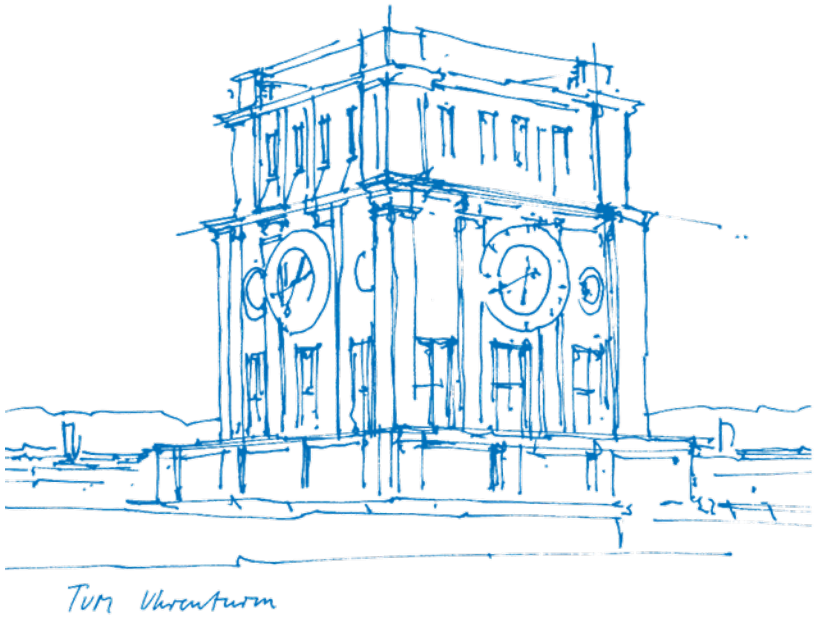
Chair of Network Architectures and Services
TUM Department of Informatics
Technical University of Munich (TUM)

Scanning the IPv6 Internet: Towards a Comprehensive Hitlist

Oliver Gasser, Quirin Scheitle, Sebastian Gebhard, and Georg Carle

Louvain-la-Neuve, Belgium, April 8, 2016



IPv6 needs a different scanning paradigm than IPv4

“0/0” approach does not work on IPv6 address space

Active security scans continue to be a valuable tool

- Discover vulnerable devices
- Assess severity and prevalence of security problems

History of IPv4 hit lists

- Opportunistic log file parsing
- Passive taps
- Repeated scans to determine stable IPs
- Scanning it all

Our approach

- Create a tailored hitlist of IPv6 addresses for security scanning

Sources for IPv6 addresses

Passive

- Large European IXP
- MWN: uplink of Munich Scientific Network with $\approx$ 100k users

$\rightarrow$ Evaluate for response rate and stability

Active

- Alexa Top 1M
- Rapid7 IPv4 rDNS
- Rapid7 DNS ANY
- DNS zone files
- CAIDA IPv6 router DNS names

$\rightarrow$ Evaluate for response rate

Traceroute

$\rightarrow$ Evaluate additional IPs learned

Passive sources

MWN: less IPs, better AS and prefix coverage, higher response rate

Characteristic	IXP	MWN
Targets	**146,722,097**	**2,687,679**
ASes	6,783	7,398
AS coverage	**66.61%**	**72.65%**
ASes unique to source	821	1,436
Prefixes	12,858	15,478
Prefix coverage	**49.87%**	**60.04%**
Prefixes unique to source	2,076	4,696
Combined AS coverage	8,219 (80.71%)	
Combined prefix coverage	25,781 (68.09%)	
ICMP response rate $\approx$	**13%**	**31%**

Active sources

Many unique ASes/prefixes for DNS ANY, ICMPv6 gives higher response rate than TCP/80 for Alexa

	Alexa Top 1M	rDNS	DNS Any	Zone Files
File size	22MB	56GB	69GB	2.6GB
Unique addresses	43,822	462,185	1,440,987	424,748
AS coverage	14.0%	47.1%	56.1%	23.3%
ASes unique to source	1	**30**	**685**	5
Prefix coverage	6.57%	26.2%	33.0%	11.62%
Prefixes unique to source	7	65	**1,379**	11
ICMPv6 response rate	**95.3%**	**68.8%**	**72.6%**	**90.6%**
tcp80 response rate	94.2%	28.4%	51.6%	88.3%
tcp443 response rate	75.8%	21.2%	27.8%	58.6%
Combined AS coverage		**7,331 (71.9%)**		
Combined prefix coverage		**12,854 (49.8%)**		

Temporal stability of IPv6 addresses

How long do observed addresses respond?

Passive sources:

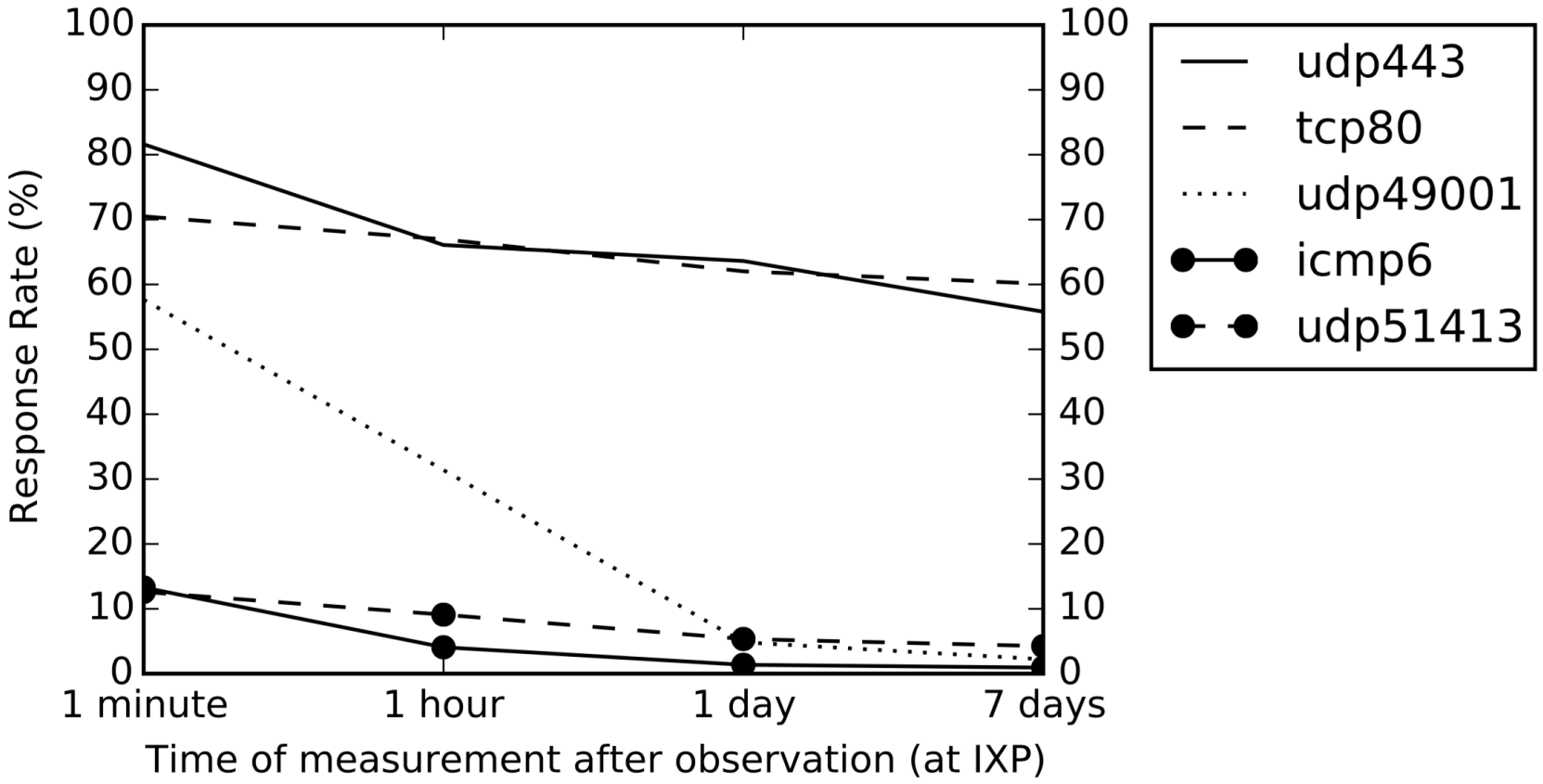
- Trigger measurement immediately after observation
- Repeat measurement using exponential back-off
- Measure observed port/protocol and ICMPv6
- zmap extended with IPv6 capabilities for high-volume scans

Active sources:

- Scan ICMPv6
- Scan tcp80 and tcp443

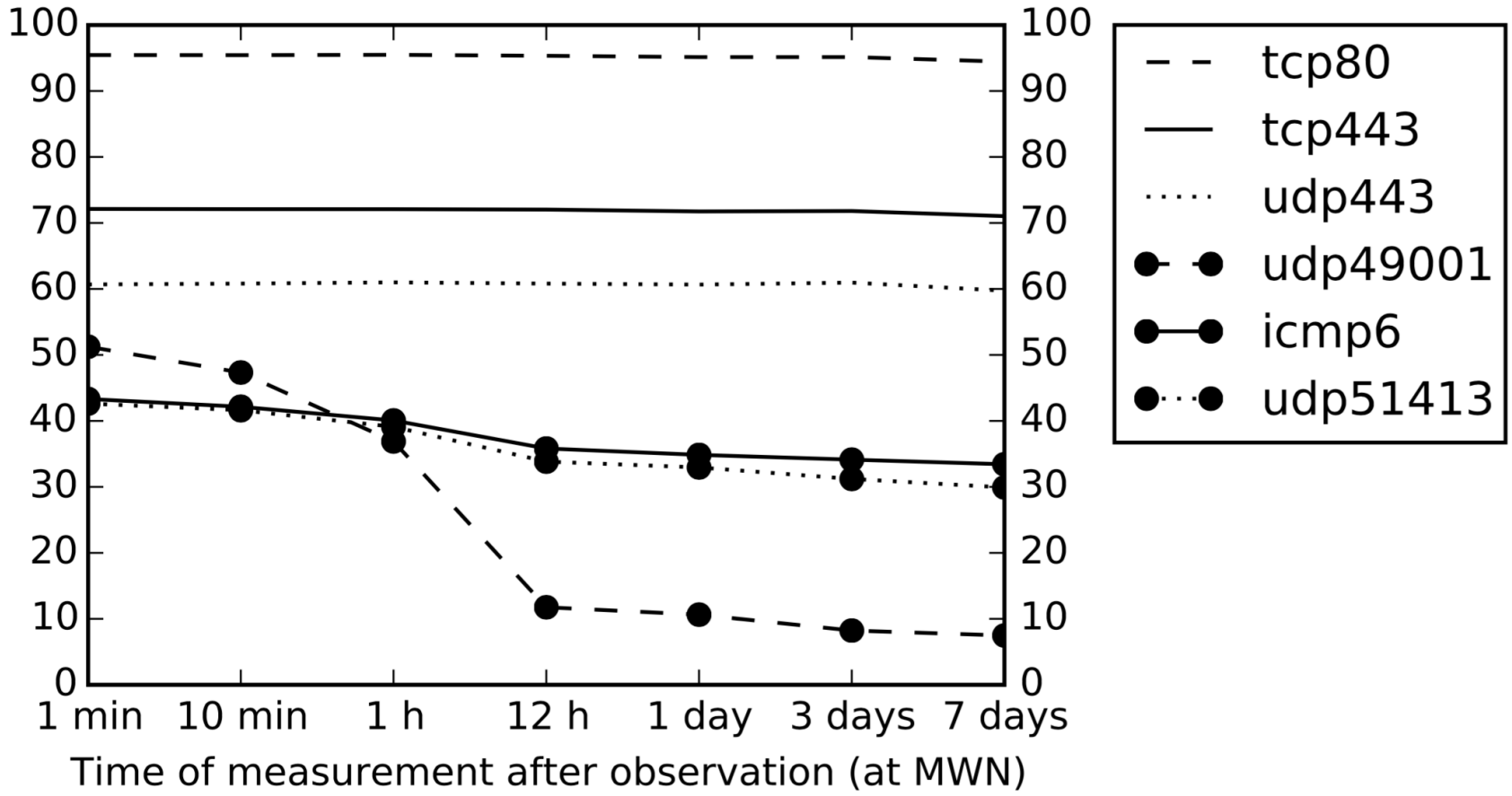
IXP response rates

Servers stable, full population with low response rate



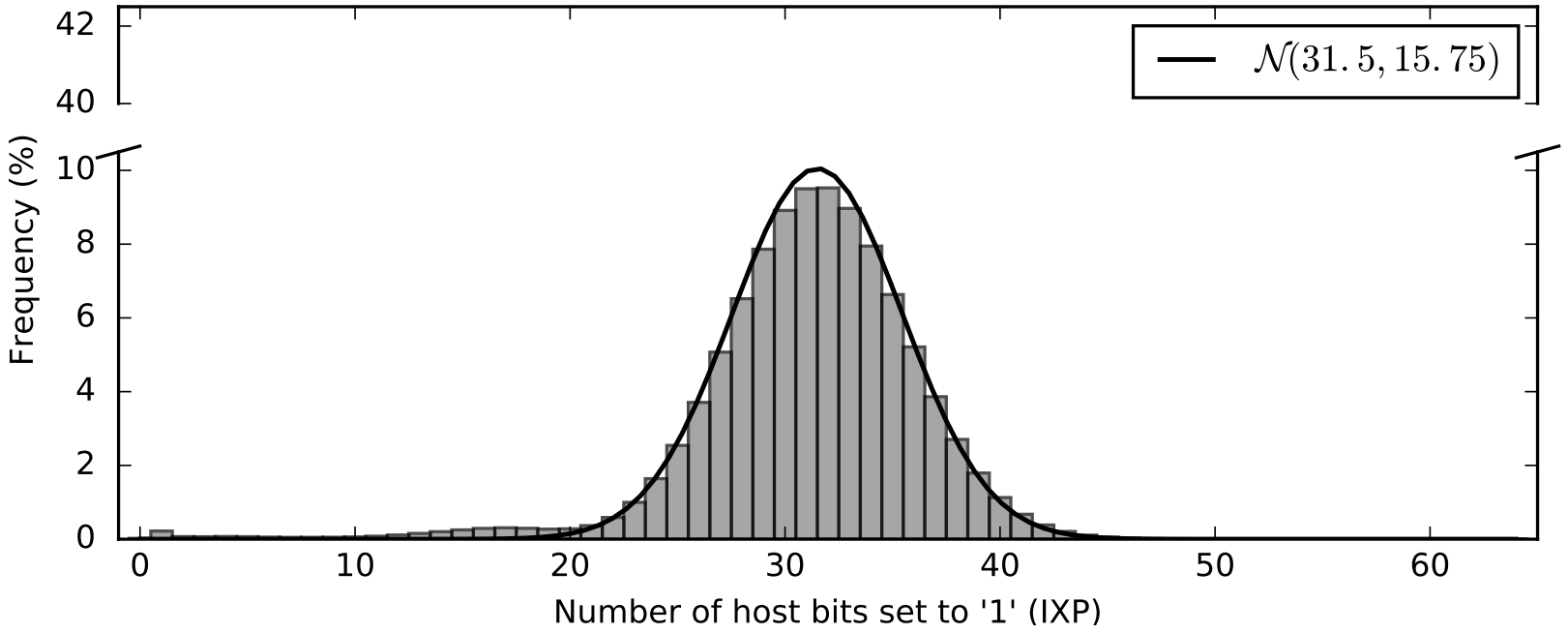
MWN response rates

Generally higher and more stable response rate

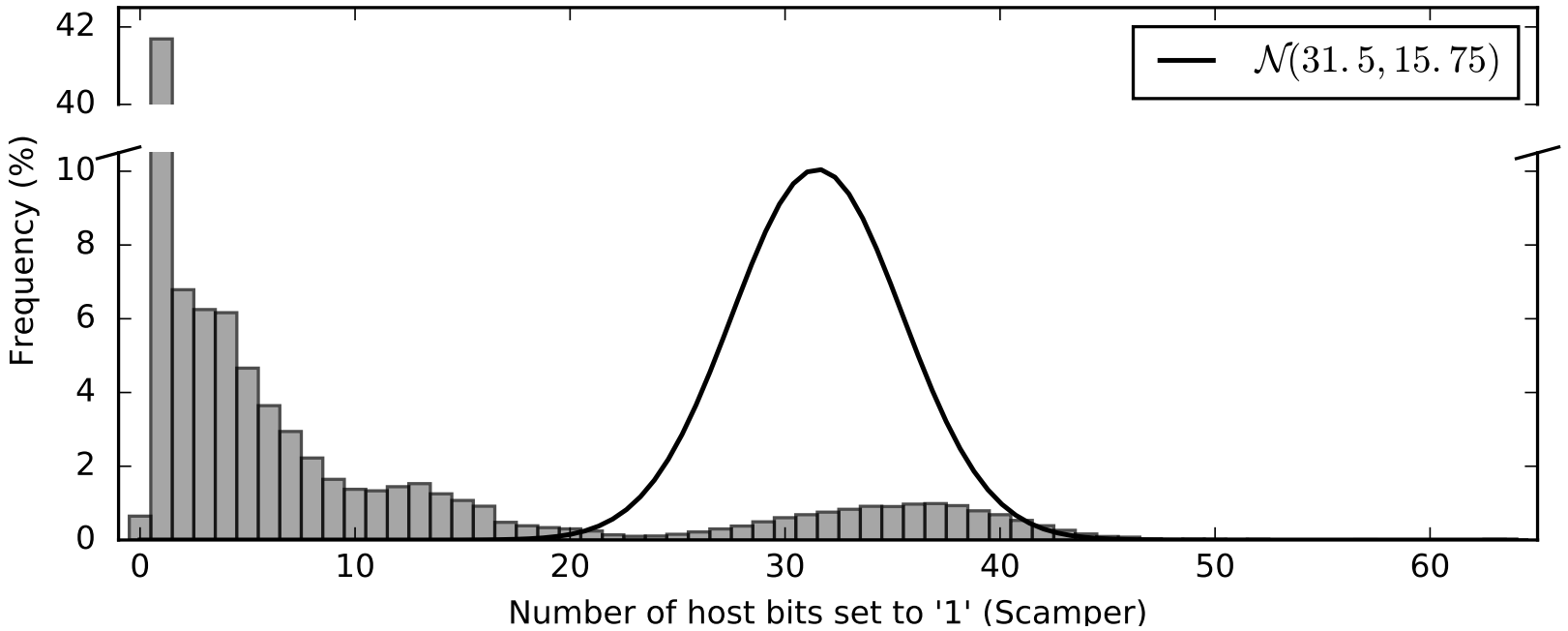


IXP Hamming weight indicates privacy extensions

- Interface ID: Commonly last 64 bits in IPv6 address
- Privacy extensions (RFC 4941): 6th bit zero, other 63 bits random
- *Central limit theorem*: 63 independent single-bit distributions $\rightarrow$ normal distribution $\mathcal{N}(31.5, 15.75)$



Traceroute Hamming weight indicates managed IP assignements



Analyzing EUI-64 IPs (`ff:fe`) in data sets

Different vendor types in IXP and traceroute data sets

TABLE IX: Top 5 vendors for EUI-64 IPs.

	IXP		Scamper	
Position	Vendor	Percentage	Vendor	Percentage
1	Samsung	30.7%	Arcadyan	28.4%
2	Apple	11.6%	Huawei	24.4%
3	Sony	5.8%	AVM	16.0%
4	Murata	5.1%	Sercomm	10.5%
5	Huawei	5.1%	Cisco	4.4%

Sources for an IPv6 hitlist

Characteristic	Active sources	Passive sources	Traceroutes	CAIDA
Targets	2,699,573	148,631,234	109,554	102,580
ASes	5,750	8,219	4,170	5,488
Announced prefixes	8,602	17,554	5,367	9,269
AS coverage	56.46%	**80.71%**	41.00%	**53.90%**
ASes unique to source	128	1,276	14	147
Prefix coverage	33.37%	**68.09%**	20.76%	**36.00%**
Prefixes unique to source	346	5,798	53	514
ICMPv6 response rate	**75.5%**	13.3%	n/a	42.0%
Combined unique IPs		**149,619,624**		
Combined AS coverage		**8,531 (83.77%)**		
Combined prefix coverage		**18,502 (71.77%)**		

Specific approach for your scan type

Most efficient sources to focus on

Internet structure finding links and nodes → passive, CAIDA, `::1` for missing prefixes

Assessing security posture many server hosts → active sources

Internet routers CAIDA, traceroute to active sources

Client protocols passive tap, but be very quick!

Finding active prefixes passive sources

Key Contributions

- Extensive evaluation of various hitlist sources
- IPv6 capabilities for zmap
- Regularly created ready-to-use hitlists

Key Contributions

- Extensive evaluation of various hitlist sources
- IPv6 capabilities for zmap
- Regularly created ready-to-use hitlists

Questions?

Oliver Gasser <gasser@net.in.tum.de>
Quirin Scheitle <scheitle@net.in.tum.de>

More information, zmap-v6 and data set available under:

`https://net.in.tum.de/pub/ipv6-hitlist/`